
Turning liquid into solid: a faucet to control the flow of liquid communication generated through social media in Botswana

Tshepho Mosweu and Mpho Ngoepe

Tshepho Mosweu

Department of Information Science, University of South Africa

lydhoss@gmail.com

<https://orcid.org/0000-0002-2144-7544>

Mpho Ngoepe

Department of Information Science, University of South Africa

ngoepms@unisa.ac.za

<https://orcid.org/0000-0002-6241-161X>

Abstract

The Botswana government uses social media platforms to communicate with its citizens. This interaction results in liquid communication which needs to be managed. Liquid communication is the type of communication that can easily go back and forth and is therefore difficult to control. This study collected qualitative data through interviews to develop a faucet to control the flow of liquid communication with a view to ensuring the trustworthiness of the content. The study established that measures to ensure the integrity of liquid communication generated through the use of social media by the Botswana government were deficient. The study recommends a framework to control and manage liquid communications.

Keywords: Botswana government, liquid communication, social media

Introduction and background

The use of social media platforms in Botswana has been reported to be high as a direct result of the government's information and communication technology (ICT) policy through which it attempts to give more people access to information (Sunday Standard Reporter 2016; Batane, 2013; Statistics

Botswana 2014). Masilo and Seabo (2015: 124) observe that the Botswana government's Facebook page titled "BWGOVERNMENT" provides updates about government programmes and policies, as well as any information that the government needs to impart to the nation. Facebook is useful in that it enables the sharing of pictures and information, status updates, posts and tags (Masilo and Seabo, 2015: 11). It should be noted here that social media platforms facilitate the movement of material from one circle of people to another, crossing the public-private lines (Duranti 2014: 7). The kind of communication that goes on social media platforms results in what is termed 'liquid communication'. Zapata (2013: ii) defines liquid communication as a type of communication that can easily go back and forth between the participants involved and that is neither restricted by time or space nor dictated by any type of social status, for example, e-mails.

With Facebook, for example, users post or share information to recipients in the network and interaction takes place as recipients make comments where the one who initially posted can respond and the communication goes on and on continually. The same post can be shared several times, resulting in liquid communication, which is difficult to manage as argued by Rogers (2015) that digital content exists in a fluid horizontal network where it may be difficult to determine authorship and or ownership. Yeo (2013) posits that even though data should be shared, each piece of data should carry evidence of its history and original context to help those who encounter it to judge its trustworthiness. To add to that, Franks (2010: 12) notes that a historically decentralised approach to records management, when combined with the rapid changes underway in the use of social media by agencies, suggests the need to consider the development of a comprehensive record and information management governance structure which directly addresses social media. Despite that revelation by Franks (2010) for the need to consider records management in social media initiatives, a recent study by Masekoameng (2018) revealed that records generated through social media were not integrated into enterprise content management at the South African Broadcasting Corporation, as this organisation did not have guidelines for managing such records. This was corroborated by Mosweu and Ngoepe (2018: 65) who advised that liquid communication generated through social media by the Botswana government should be properly managed to avoid questions over trust, privacy and security of information.

Botswana government social media pages are administered by the Botswana Government Communications and Information System (BGCIS), a division under the Office of the President. This office was established to ensure that the Botswana government communicates appropriate information in a timely, authoritative, coherent, coordinated and proactive manner (Botswana government 2020). It is important to note that despite the acknowledged

utilization by governments of social media platforms to transact, there seems to be a lack of coordinated efforts to manage social media records around the world. A study done by InterPARES (2016: 76) in America and Canada indicated that while participants of the research generally acknowledged that communication in social media were records, little effort was made to manage social media content. Goh, Duranti and Chu (2012: 2) report that to deal with some of the challenges that come with digital records management, some countries such as Australia have updated their legislation related to privacy, data protection and intellectual property.

The literature shows that most countries have not been proactive in amending relevant legislation to accommodate the governance of social media records, but rather have policies and guidelines in place for the management of digital and social media records (Parer 2002: 2; Jaeger, Bertot and Shilton 2012: 11; Goh, Duranti and Chu 2012). This is also the case in Botswana, as the archival legislation relies on a wide definition of a record that. It intends to cover as many forms of records as possible in as many media as possible including those which are generated through social media. In legal terms, wide coverage is mostly encouraged so that other aspects may not be subjected to non-protection owing to their falling outside the ambit of the legislation (Ngoepe and Saurombe 2016).

Although Goh, Duranti and Chu (2012: 2) acknowledge that several national archives, including Australia and the United States, have issued policies and guidelines on the outsourcing of digital data and how to manage records in a cloud computing environment, they are sceptical where these policies and guidelines are not supported by strong archival legislation, as legislation is the highest form of public policy. Most countries with social media policies for government are found in the developed world such as the United States where the National Archives and Records Administration has issued Bulletins on Guidance on Managing Records in Web 2.0/Social Media Platforms (2016), the New South Wales Archives repository has Government Social Media Policy and Guidelines (2016) and, at a lower level, in Africa where the Nigerian government, through the National Information Technology Development Agency (NITDA), has the Draft Framework and Guidelines for the Use of Social Media Platforms in Government Establishments (2017).

Research problem

Information generated through social media can be shared or re-posted beyond the control of the creating agency and in this way raises issues of trustworthiness of the resulting communication. For example, if one posts on

Facebook and one of the followers shares the post, if the original post is updated, this does not affect the shared post. The Botswana government made use of the advantage of social media to increase access to, and usage and awareness of their services (Masilo and Seabo 2015; Statistics Botswana 2014; Vision 2016 Council 2015). In the process, records are created and posted on social media, including notices of public meetings, public service announcements, press releases, live speeches and requests for service.

Preliminary research has shown that despite the use of social media platforms to communicate government decisions, liquid communications generated through these platforms are often not managed (Mickoleit 2014) and, hence, integrity controls are not implemented. This may be attributed to the fact that those who create, manage, appraise, control and preserve records generated in cloud environments encounter problems related to ownership, provenance and jurisdiction, among others, as they remain responsible for such materials without control and are accountable without knowledge (Duranti 2015).

Furthermore, social media users have little control over how and where the documents are stored in the cloud, who has control and jurisdiction, who can access them or how secure they are, putting their trustworthiness in question (Mitchetti 2017: 232). There is a need to ensure the trustworthiness of liquid communication as social media posts may serve legal and compliance purposes during e-discovery (Franks and Smallwood 2014:264-254; Madhava 2011: 33). Moreover, in the digital environment, authenticity is an integral value that must be protected over time and across technological changes (Rogers 2015: 2). To ensure the integrity of information, the information assets generated by or managed for the organisation need to have a reasonable guarantee of authenticity and reliability (Association of Records Managers and Administrators (ARMA) 2017). Hence, this study sought to develop a faucet to control the flow of liquid communication generated through social media in Botswana.

Research questions

This study aimed to develop a faucet to control the flow of liquid communication generated through social media in the Botswana Public sector. The specific questions of the study were the following:

1. What procedures are in place to support the generation and management of liquid communication?
2. What measures are in place to ensure the authenticity of liquid communication?
3. What faucet can be suggested to control and manage liquid communication?

Theoretical framework

The theoretical framework for this study is based on the Association of Records Managers and Administrators (ARMA) Generally Accepted Recordkeeping Principles (ARMA, 2017). Hagmann (2013: 232) contends that these principles take account of the foundations of relevant records and information management standards such as the Records Management ISO 15489 standard as well as best practice and legal and regulatory requirements. According to ARMA (2017), the principles constitute a generally accepted global standard that identifies the critical hallmarks and a high-level framework of good practices for information governance. Published by ARMA International in 2009 and updated in 2017, the principles are grounded in practical experience and based on extensive consideration and analysis of legal doctrine and information theory. They are meant to provide organisations with a standard of conduct for governing information and guidelines by which to judge that conduct. The principle of integrity and protection are particularly relevant to answer the research questions for this study. The principle of integrity according to ARMA (2017), pronounces that where there is an information governance programme in place, the information assets generated by or managed for the organisation should have a reasonable guarantee of authenticity and reliability. On the other hand, the principle of protection requires that there should be a reasonable level of protection of records and information that are private, confidential, privileged, secret, classified, and essential to business continuity or that otherwise require protection (ARMA 2017).

The concept of liquidity in archives and records management

Traditionally, in the field of archives and records management, a record was based on fixity and stability in a material sense (Jeurgens 2017: 205). As espoused by the social theorist, Bauman (2000) in his book *Liquid modernity*, the society has moved away from a solid hardware-focused modernity to a liquid software-based modernity. Ketelaar (2017) alludes that as much as archivists apply archival methods specific to their discipline, they are increasingly profiting from what other disciplines can offer in conceptual and theoretical understanding of archival phenomena. Indeed, even in the archives and records management profession, the traditional practices and paradigms in the field have changed in the liquid modernity. It is with this background that this study applies the concept of liquidity to highlight possible solutions to challenges brought about by social media in terms of trustworthiness of liquid communication. It has been emphasised by Thompson (2016: 33) that strategies

for preserving social media are largely adaptive, relying on established practices for analogous types of digital content. Owing to that, Mitchetti (2017: 235) posits that the archives and records management field has begun to implement and develop services from cloud-based services such as providers of email and social media services.

Jeurgens (2017: 205) believes that the advent of social media has brought a predicament to the archives and records management profession as the profession cannot reliably say what a record is as it converges with data, documents, information and the archives. This study acknowledges the different definitions of a record in professional literature, noting the differences from a traditional definition of a record to a definition of a record in liquid times. The International Records Management Trust (IRMT) (2009) defines a record as documentary evidence, regardless of form or medium, created, received, maintained and used by an organisation (public or private) or an individual in pursuance of legal obligations or the transaction of business. According to InterPARES Trust (2018), it is a document made or received and set aside in the course of practical activity. On the other hand, the ISO 15489 (2016:4), states that a record, regardless of form or structure, should possess the characteristics of authenticity, reliability, integrity and usability to be considered authoritative evidence of business events or transactions and to fully meet the requirements of the business.

According to proponents of the records continuum theories, a record status does not have to be determined by crossing the threshold of record-keeping systems, as even ephemeral records and informal communications have evidential characteristics that qualify them as records (Yeo 2015). Even for legal purposes, as stated by Yeo (2015), because the selection decisions are imperfect, all records can be subject to discovery or disclosure (including drafts, casual messages, and records that survive by coincidence). Even though the form of digital objects such as liquid communication may be neither fixed nor stable in the traditional sense as they exist in a fluid horizontal network where authorship and ownership may be difficult to determine, and their diverse range may not conform to the definition of “record”, they still need to be maintained and preserved with their authenticity and reliability protected (Rogers 2015: 8).

Trustworthiness and protection of liquid communication

By its nature, liquid communication tends to be technically volatile; hence, it has trustworthiness complications (Mosweu and Ngoepe 2018: 63). The main contention here is how to protect the trustworthiness of liquid communication generated under generally insecure environments. ARMA (2017) states that information governance programmes shall be constructed so that the

information generated by or managed for the organisation has a reasonable and suitable guarantee of authenticity and reliability. Trustworthiness here means that the records generated in the process are complete and authentic. In records management, according to the International Council on Archives (ICA) (2016), the term often used to describe record qualities as reliable, authentic and accessible is 'integrity' which means the records are whole and without corruption. Yeo (2015: 316) highlights that in digital environments, "documents" may be declared as records when they cease to be volatile and are captured in an electronic records management system. However, he does acknowledge the view by proponents of the continuum model that records status is not determined by crossing the threshold of such a system, but even informal communications have evidential characteristics that qualify them as records. Cloud computing service agreements for social media or free online storage carry greater risks to the security of information (Duranti and Rogers 2014: 5). As such, the Botswana government should have measures in place to deal with the trustworthiness of liquid communication generated through social media in government. The ICA (2016: 13) argues that as records are the product of work processes, it follows that the quality and trustworthiness of records depend on the quality and integrity of the work processes that generate them, which means if the work processes are poorly defined or inconsistent or not followed correctly, the records produced may not be adequate.

Jansen and Grance (2011: 25) warn that the growing availability and use of social media, personal Webmail, and other publicly available sites are a concern since they increasingly serve as avenues for social engineering attacks that can negatively impact the security of the client, its underlying platform and cloud services accessed. One way to deal with such threat as suggested by ARMA (2017) is that information governance should ensure a reasonable level of protection of records and information that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection under the Principle of Protection. Smallwood (2014: 32) posits that this principle applies equally to physical and electronic records, each of which has unique requirements and challenges. The International Standards for Records Management, ISO 15489 (2016: 7), requires that measures such as access controls, monitoring, agent validation and authorised destruction should be implemented to prevent unauthorised access, alteration, concealment or destruction of records. Information about the controls that were applied to a record and when they were applied should be recorded in the record's process metadata. Rogers (2015: 6) also advises that organisations may use digital diplomacies, based on a foundation of traditional diplomatic principles to help them identify digital records through their metadata and determine what metadata need to be captured, managed and preserved. Rogers (2009: 9)

explains digital diplomacy as a theory which provides a model of a “record” and a means of understanding and defining record authenticity as well as the elements that comprise it.

The issue of trustworthiness of liquid communication has become paramount in the era of post-truth, disinformation and fake news where it has become easier to create and share information beyond the creator’s control, such that Evans (2017) is of the view that the issue of fake news has continued to increasingly tarnish the image of social media. Duranti (2017) argues that the fact that people nowadays are always connected online has led to a situation where falsehoods and incorrect information circulate mainly through social media at rates unimaginable only a few decades ago. The question now becomes “How do we maintain the authoritative role of records as evidence in the digital era?”

Of recent concern has been the spreading of fake news through social media in the wake up of the novel coronavirus (Covid-19). Douek (2020) asserts that the coronavirus pandemic has forced tech providers to moderate social media content in order to combat fraud and misinformation about the virus, elevate authoritative content on the platforms and share critical updates in coordination with government healthcare agencies around the world. On the other hand, many countries are adopting laws and regulations to combat the spread of fake news on the virus through social media. In Russia, lawmakers are reported to have rushed a bill through all three readings in just one day to approve fines of up to \$25,000 and prison terms of up to five years for anyone who spreads what is deemed to be false information and disinformation about the outbreak, sparking concerns that the government is using the laws to suppress alternative points of view (Litvinova 2020). In the Philippines, the Philippine National Police are reported to have filed criminal complaints against reporters for spreading “false information” about the country’s Covid-19 status by implementing the newly enacted emergency Bayanihan to Heal as One Act, which criminalises the dissemination of “false news” (CPJ 2020). There have been new laws across Southeast Asia meant to bar the dissemination of fake news about the coronavirus, with bloggers in at least two countries facing possible prison time for postings as short as one sentence, raising fears on the curtailment of free speech and freedom of the press (VOA News 2020). In Africa, countries like South Africa, Zimbabwe and Botswana also have recently enacted laws and regulations meant to combat the spread of fake news about Covid-19 through the use of social media (Karrim 2020; The Standard, 2020; Botswana Communications Regulatory Authority 2020). Authenticating this liquid communication is a challenge as Yeo (2013) asserts that information needs higher standards of verification in digital realms than in the paper world.

Research methodology

A qualitative approach with a case study research design was adopted to develop a faucet to control the flow of liquid communication generated through social media in Botswana. The sample of this study was purposively selected from four Botswana government organisations, that is, Botswana Government Communications and Information System (BGCIS), which is responsible for social media in the government of Botswana and other stakeholders such as the Department of Information Technology (DIT), Botswana National Archives and Records Services (BNARS) and the Botswana Communication and Regulatory Authority (BOCRA) that are also involved in social networks and government information. These are the main authority as it concerns information management in the country. Government ministries that do not have information management as their primary mandate are not covered by this study. Nineteen participants were targeted based on their experience and knowledge of the usage of Botswana government social networks and information management in the country and out of that twelve were available and interviewed. Nonetheless, the interviewed participants generated data that were considered sufficient to make generalisations in this study as it is explained by Creswell (2012: 206) that in qualitative research, the researcher selects people or sites that can best help in understanding the principal phenomenon. The government social media pages which were examined during the data collection period, between November 2017 and April 2018, include Facebook, Twitter, YouTube and Instagram. The participants were given code names as per their institution, namely, BGCIS, BNARS, DIT, BOCRA and a unique number in addition to the institution abbreviation. Data were coded and analysed through thematic analysis.

Research findings and discussion

This section presents the findings of the study as obtained through interviews to examine measures put in place to maintain the authenticity of liquid communication generated through the use of social media by the Botswana government. The objective was informed by the ARMA principles of integrity and protection. The principle of integrity demands that the information generated by or managed for the organisation should have a reasonable and suitable guarantee of authenticity and reliability, while the principle of protection requires that there should be a reasonable level of protection of records and information that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection (ARMA 2017). The sub-themes that emerged under this objective included the processes undertaken for introducing new records-generating systems for liquid

communication, precautionary measures put in place to ensure that liquid communication remains authentic, auditing of integrity controls of liquid communication, frequency of incidents of inappropriate information disclosure as well as goals related to liquid communication protection. These sub-themes were principally addressed by participants from the BGCIS office as the administrators of government social media pages. Other stakeholders such as BNARS, DIT and BOCRA played an insignificant role in government social media efforts which went against the assumption of this study.

Procedures for introducing new records-generating systems

The participants were asked to talk about the process they undertake to introduce new records-generating systems for liquid communication; that is, capturing their metadata and meeting other authenticity requirements, including the chain of custody. In response to this question, participant BGCIS1 said, “Our junior officers, assistant principal relations officers, develop content that is both news and live coverage. They prepare draft content and schedule it to give the upper-level responsibilities to approve it before it can be published.” This is despite the fact that participants BGCIS2 and BGCIS4 said no processes had been undertaken to introduce new records-generating systems for social media records. While participant BGCIS3 said that as PROs, they only post information that has already been authorised by the directors of different government departments. This is also corroborated by participant BGIS5 who said, “The information we post comes from government departments. The process is mostly at the departments. That is where various departments initiate information, go through the PRO at the department, then the director, before it comes to us, the PR department, to post. When it comes to us, we just post it, because it has already gone through the processes. This process helps us because the information has already been verified and vetted, we can only correct grammar or put the message in a catchy way.” The responses by the participants indicated that the processes for introducing new records-generating systems were weak, which calls for a governance framework for liquid communication as suggested by this study. Through the proposed framework, the capturing and authenticating of liquid communication generated through the use of social media can be ensured.

As this study established that the use of social media by the Botswana government was mainly on a laissez-faire and experimental basis, it also found there was not much the participants could say about the processes they undertake to introduce new records-generating systems for social media records, that is, capturing their metadata and meeting other authenticity requirements. Although some participants acknowledged that there were no distinct processes undertaken for introducing new records-generating systems for social media

records, the PROs revealed that the APROs were the ones who developed content, prepared draft content and scheduled it to give the upper-level responsibilities to approve it before being published. Moreover, the PROs only posted information on social media after it has been verified, vetted and authorised by the government departments concerned. Unfortunately, these processes were not formally documented for records integrity purposes. According to ISO 15489 (2016:6), records systems should be able to apply records controls, carry out processes for creating, capturing and managing records and support the creation and maintenance of logical relationships between records content and metadata for records.

Franks (2013) posits that when there is a formal, defined process for introducing new records-generating systems and the capturing their metadata as well as other authenticity requirements, the organisation's goals related to integrity would have been met. The same author continues to state that, in that way, the organisation can consistently and confidentially demonstrate the accuracy and authenticity of its records. In addition to documenting such processes, Latham (2014:6) argues that as social media platforms are not typically designed for record capturing and management, there is a need to investigate and document platforms used by the government and the type of records being created, and to devise strategies to capture and preserve required records appropriately.

This study established that crucial stakeholders in records and information management such as BNARS, DIT and BOCRA were not directly participating in government social media efforts leaving the BGCIS office to manage the whole process of social networking by the Botswana government. The participants from these offices were questioned on their roles concerning the use of social media by the government. Concerning BNARS, participant BNARS1 stated that "BNARS has no mandate with regard to the adoption of social media by the government as it has no policy governing the use of social media". However, the BNARS participants pointed out that BNARS has its own social media page and, according to participant BNARS5, the department "has developed its own social media page on FB [Facebook] which, from time to time, does give a snapshot of events which happened in a particular month, or just which gives Botswana a hint by providing pictures on its page". This revelation shows an individual decision for the department which does not assist the entire government's social media efforts. BOCRA1 revealed that BOCRA did not partake directly in governments social media efforts but the authority "has a mandate to listen to and resolve complaints from stakeholders and consumers, including complaints about the use of the internet". The role of the DIT was also limited on social media as participant DIT1 indicated that the "DIT is mandated, among other things, to provide internet connection for both

the government community and the school community” among other duties which are not directly correlated with government social media efforts.

The authenticity measures for liquid communication

When asked what were the precautionary measures put in place to ensure that social media records remain authentic, participant BGCIS1 said, “There are two levels of back-end user rights, which are the author, the lower-level responsibility, the super administrator, and the upper-level responsibility. The author level is performed by junior officers such as APROs or interns. The super administrator level is performed by senior officers who create users on the government social media pages and assign levels of responsibilities.” In response to the same question, participant BGCIS2 said that the question is not applicable in their case as they follow a communications process that only PROs prepare the information used to update government social media pages. Participant BGCIS3 said only two officers were appointed to be administrators as a precautionary measure for security purposes. It was important to note participant BGIS5’s response which stated that the government of Botswana had not reached that level where precautionary measures could be put in place to ensure that social media records remain authentic since they were not taken as records in the first place.

The liquid nature of records generated through the use of social media requires that precautionary measures be put in place to ensure that the records remain authentic. The use of diplomatics to assess the authenticity of a variety of documentary forms has led to the application of diplomatic principles in the digital environment and the development of a specialised field of “digital diplomatics” developed at the University of British Columbia (UBC) through the International Research on Permanent Authentic Records in Electronic Systems (InterPARES) research projects (Rogers 2015:7). Governance of liquid communication requires that practices should be in place to trace authorised annotation, addition to or deletion of a record and that these should be explicitly indicated and traceable (Franks 2010:28).

The International Records Management Standard ISO 15489-1 (2016) states that a record, regardless of form or structure, should possess the characteristics of authenticity, reliability, integrity and usability to be considered authoritative evidence of business events or transactions and to fully meet the requirements of the business. The integrity of records refers to record qualities as being reliable, authentic and accessible in that they are whole and without corruption (International Council on Archives 2016). The principle of integrity demands that the information generated by or managed for the organisation should have a reasonable and suitable guarantee of authenticity and reliability, while the

principle of protection requires that there be a reasonable level of protection to records and information that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection (ARMA 2017). This means the government of Botswana need to put measures in place to ensure the authenticity and reliability of their social media content as this study revealed that government social media content was not managed as records.

Audit of integrity controls for liquid communication

The participants were asked whether the controls for liquid communication were audited reliably and systematically and to comment on the process of the audit. This question included how often a social media content audit was done and asked the participants to state any continuous improvements that were normally undertaken. In response, participant BGCIS1 said, “There are two publishing workflows. The configuration matrix is such that junior-level prepares and loads draft content. This level cannot publish, as the publishing rights do not allow him/her to transact at that level. In the matrix, there is the super administrator who creates users and allocates rights in the publishing workflow. Everyone in the publishing workflow changes their passwords periodically by following the Facebook security password creation policy.” Participants BGCIS2, BGCIS3 and BGCIS4 said there were no audits undertaken for integrity controls of social media in the Botswana government. According to participant BGIS5, as the PROs, they often met and discussed the audit reports from government social media pages mostly “for impact on the number of people reached, popularity of the posts, what went wrong, why it was not popular, what can we do to make it popular”. This answer was evidently not relating to the audit of integrity controls of social media records. This was understandable as the PROs had indicated in the study that they used social media for publicity purposes and were not concerned with governing liquid communication.

The main aim of maintaining the authenticity of the records is to make sure that the nature of any actions undertaken upon the records are documented, whether through additions of integrity metadata or by compilations of reports to provide a kind of audit trail on what has happened to the records since their creation (Duranti and Preston, 2008:212). Audit processes are crucial, particularly in the process of capturing and managing of liquid communication. The International Records Management Standard ISO 15489 (2016:13) states that processes for creating, capturing and managing records rely on up-to-date records controls. Therefore, records controls should be regularly reviewed where versions of records controls that have been superseded should be retained and managed as

records in accordance with requirements identified from the appraisal. The ARMA principle of accountability requires there be an audit process that includes records management requirements. According to Franks and Smallwood (2014:30), this audit process must involve assigning sufficient levels of accountability as well as identification and addressing any accountability deficiencies.

Frequency of incidents of inappropriate information disclosure or loss

The participants were also asked to comment on any incidents they ever had where information was disclosed or lost inappropriately or inadvertently and how often they had experienced such situations. All the PROs and participants BGCIS1, BGCIS2, BGCIS3, BGCIS4 and BGIS5 said they have not experienced any situation where information was disclosed or lost inappropriately, with participant BGCIS2 adding that if ever there had been such cases, inappropriate information was posted by clients and not by the government social media pages administrators. Despite these revelations by the participants, incidents of inappropriate information disclosure or loss are inevitable with the use of social media platforms (Franks and Smallwood 2014). As a result, this study proposed a faucet to control the flow of liquid communication generated through social media in Botswana to avoid the frequency of such incidents.

As social media has proved to be the Wild West of collaboration and communication with its vulnerabilities where rules change almost all the time, incidents of inappropriate information disclosure are not uncommon (Franks and Smallwood 2014:258). Franks and Smallwood (2014) continue to explain that these risks are prevalent where there are no social media policies or a lack of monitoring and enforcement. The participants were also asked to comment on any incidents they ever encountered where information was disclosed or lost inappropriately or inadvertently, and how often they had experienced such a situation. In reply, they all indicated that it has never happened with government social media pages. They revealed that incidents of posting inappropriate information have been observed from the users. Nonetheless, it is crucial as argued by Yeo (2015) to capture records within a formal records management system as that assists in securing the records against loss, damage, alteration, or premature destruction as well as their future access.

Access controls responsibilities

The participants were asked to comment on the responsibilities to assign access controls. Although participants BGCIS2, BGCIS3 and BGCIS4 said the

permanent secretary in the Office of the President was the one who assigned access controls, participants BGCIS1 and BGCIS5 indicated that it was the PROs who did the job. In explaining this, participant BGCIS5 said, “The super administrator, who is the most senior, in our case is the principal public relations officer, creates users on government social media pages and assigns access controls for security purposes.” All the participants revealed that the government of Botswana did not have documented processes to guide the transfer or disposition of social media records. As a consequence of this, processes for suspending disposition in the event of investigation could not be established in this study. To enlighten this situation, BGCIS5 said, “There are no documented processes as we never took social media content as records.” But researchers such as Franks (2010), Iron Mountain (2012) and Masekoameng (2018) warn that the failure to put measures in place to manage social media content will eventually result in records management challenges and great costs for the government.

To protect liquid communication generated through the use of social media by the Botswana government, one of the steps to be taken is assigning access controls to prevent unauthorised access and disclosure. The ISO/IEC 27001:2013, Information technology – Security techniques – Information Security Management Systems – Requirements, states that access controls are one part of a broader approach to securing information through an information security management system. The super administrators (upper level), in relation to the deputy permanent secretary communications and the PPRO, were mentioned as having the responsibilities to create users on government social media pages and assigned access controls for security purposes by the study participants. The International Records Management Standard ISO 15489 (2016:13) requires that records controls should be developed to assist in meeting records requirements. These controls include the following:

- a) metadata schemas for records
- b) business classification schemes
- c) access and permissions rules
- d) disposition authorities.

According to the ISO 15489 (2016:13), records controls may be designed and implemented in a variety of forms, depending on the technological and business environment. Their design and implementation should take account of the nature of the records systems with which they need to interact.

Proposed faucet to control and manage liquid communication

This study has revealed that even though the government of Botswana was active on social media, thereby generating liquid communication, there were no measures for the capturing of liquid communication. As liquid communication generated through the use of social media by the government is evidence of its official business, it should be captured and managed according to records management requirements, as supported by the existing legal framework. As rightly stated by Yeo (2015), capturing records within a formal records management system assists in securing them against loss, damage, alteration, or premature destruction, besides supporting their continuing accessibility. The moment an organisation is satisfied that the liquid communication generated through social media has the above characteristics, the liquid communication should be captured and managed according to the organisation's records management requirements. The communication that goes on between the government and the citizens should be retained for reasons of accountability and transparency under records management requirements and legal requirements. Some social media platform such as Facebook, LinkedIn and Twitter have export capabilities built into their systems which convert content into files that can be available for download. The Public Records Office Victoria (2013) suggests the type of social media posts to be captured may include the original post from the social media site, responses to the original post, if any are received, relevant posts identified when monitoring social media sites, and the content republished by an organisation when the content has come from elsewhere. This study proposes an implementation framework to capture and manage liquid communication in order for organisations to comply with the records management and legal requirements as depicted in Figure 1.

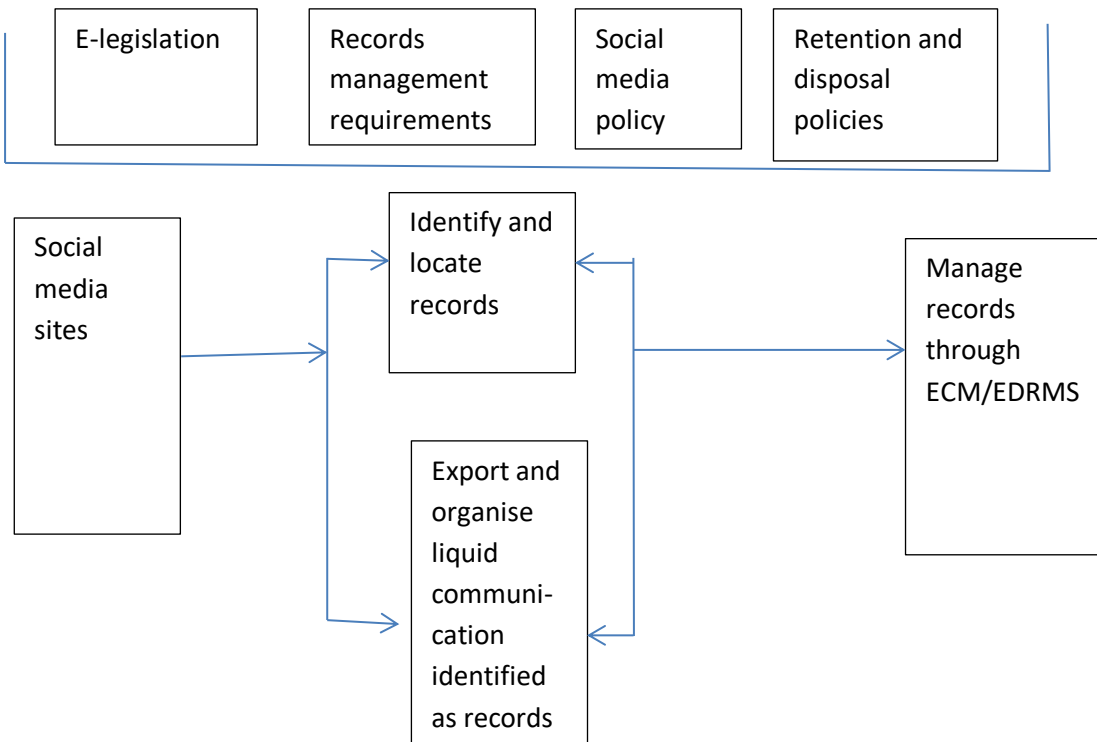


Figure 1: Proposed framework for the capture of liquid communication (Researchers 2020)

Drawing from these study findings and the Library of Congress (2018) digital archiving process, the proposed framework provides the following key steps to be taken to capture liquid communication by the Botswana government:

1. Identify the social media platform
 - a) Locate all content liquid communication on the social media sites.
 - b) Include both the current information and any older (archived) content.
2. Select liquid communication classified as records according to records management requirements
 - a) Pick individual pieces of information or select the whole page or site.
3. Export the selected information
 - a) If saving a limited amount of information, you can use the “save as” command in your web browser to export the site as individual files.
 - b) If saving entire pages or sites, consider automatically exporting them as a series of linked files.
 - c) Save metadata for your content information, such as site name or date created.
4. Organise the information
 - a) Give individual files descriptive file names.

- b) Create a directory/folder structure on your computer to store the saved information.
- c) Write a brief summary of the directory structure and its files.
- 5. Manage liquid communication according to your records management requirements
 - a) Save copies on separate media such as DVDs, CDs, portable hard drives, thumb drives or internet storage.
 - b) Put a copy of the summary description with your important papers in a secure location.
 - c) Create new media copies every five years or when necessary to avoid data loss.
 - d) Provide an audit trail for each stage of the captured information.

The legal and records management requirements may vary from country to country according to the existing laws and established records management requirements that regulate information governance in each country.

Notwithstanding the above, the governance of liquid communication requires the existence of a social media policy to ensure a formalised process for the governance of liquid communication. This policy should regulate the control, creation, receipt, transmission, maintenance and disposition of liquid communication. It is through this policy that a records management system is established to keep track of social media activities. The social media policy would facilitate compliance with the national archives and records services' guidelines for records management and archiving as well as compliance with applicable laws and other binding policies in the country.

Conclusion

The findings of this study have shown that liquid communication generated through the use of social media with a reasonable and suitable guarantee of authenticity and reliability needs to be considered authoritative evidence of government business. To ensure the trustworthiness of liquid communication generated by the Botswana government, the government should put measures in place to ensure that liquid communication is protected against unauthorised addition, deletion, alteration, use and concealment through audit trails. Owing to its fluidity, liquid communication should be captured and managed according to the government's electronic records management systems. All this should be done in the presence of the established legal and policy framework to fulfil the legal requirements. In that way, legal and compliance risks embedded in the use of social media are reduced while ensuring the future accessibility of liquid communication. It has been established that although the BNARS has a legislative and regulatory mandate towards government agencies to collect, preserve and make accessible the nation's documentary heritage, it was not

involved in the management and preservation of liquid communication. For the suggested faucet to turn liquid content into solid for the purpose of preservation, the BNARS must be involved in the management of liquid communication generated by the Botswana government throughout the entire life cycle.

References

- Association of Records Managers and Administrators (ARMA). 2017. *Generally accepted recordkeeping principles*.
https://cdn.ymaws.com/www.arma.org/resource/resmgr/files/Learn/2017_Generally_Accepted_Reco.pdf Accessed 2 June 2018.
- Batane, T. 2013. Internet access and use among young people in Botswana. *International journal of information and education technology* 3(1): 117-119.
- Botswana Communications Regulatory Authority. 2020. Public notice. Publishing, forwarding or creating false information using online platforms is an offence. <https://www.bocra.org.bw/public-notice-3> Accessed 13 April 2020.
- Botswana government. 2020. Ministry for Presidential Affairs Governance and Public Administration.
<https://www.gov.bw/ministries/ministry-presidential-affairs-governance-and-public-administration> Accessed 2 April 2020.
- Committee to Protect Journalists (CPJ). 2020. *Two reporters charged for spreading “false information” about COVID-19 in the Philippines*.
<https://cpj.org/2020/04/two-reporters-charged-for-spreading-false-informat.php> Accessed 13 April 2020.
- Creswell, J.W. 2012. *Educational research*. Los Angeles: Sage Publications.
- Douek, E. 2020. Covid-19 and social media content moderation.
<https://www.lawfareblog.com/covid-19-and-social-media-content-moderation> Accessed 13 April 2020.
- Duranti, L. 2014. *InterPARES Trust. Observations about records in the cloud & progress report*.
https://interparestrust.org/assets/public/dissemination/Duranti_20140526_ProjectReport97_2004.ppt Accessed 23 February 2020.
- Duranti, L. 2015. Special issue: data, records, and archives in the cloud. *Canadian journal of information and library science* 39(2): 91-96.

Duranti, L. 2017. *An infrastructure for truth entrusting digital facts to archival theory*. <http://www.alaarchivos.org/wp-content/uploads/2017/12/Magistral-Luciana-Duranti.pdf> Accessed 1 June 2019.

Duranti, L. and Preston, R. 2008. *Research on permanent authentic records in electronic systems (InterPARES) 2: experiential, interactive and dynamic records*.
http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf
Accessed 13 June 2019.

Duranti, L. and Rogers, C. 2014. *Trust in online records and data*.
https://www.researchgate.net/publication/290042093_Trust_in_Online_Records_and_Data Accessed 2 March 2019.

Evans, L. 2017. *Social media presence in a post-truth world*.
https://sustain.ubc.ca/sites/sustain.ubc.ca/files/Sustainability%20Scholars/2017_Sustainability_Scholars/Final_Reports/Social%20Media%20Presence%20in%20a%20Post-Truth%20World_Evans_%202017%20SS.pdf Accessed 1 June 2019.

Franks, P. 2010. *How federal agencies can effectively manage records created using new social media tools*.
http://observgo.quebec.ca/observgo/fichiers/57504_GRI%201.pdf Accessed 15 February 2020.

Franks, P. 2013. *Electronic records management*.
https://www.statearchivists.org/files/7014/7209/3942/Electronic_Records_ManagementPresentation-Franks.pdf Accessed 15 July 2019.

Franks, P. and Smallwood, R.F. 2014. Information governance for social media. In: Smallwood, R.F. ed. *Information governance*. New Jersey: John Wiley & Sons, pp. 253-269.

Goh, E., Duranti, L. and Chu, S. 2012. Archival legislation for engendering trust in an increasingly networked digital environment. Paper presented at *A climate of change: International Council on Archives Congress*, Brisbane, 20-24 August 2012.

Hagmann, J. 2013. Information governance – beyond the buzz. *Records management journal* 23(3): 228-240.

International Council on Archives. 2016. *Managing metadata to protect the integrity of records*.

<https://www.ica.org/sites/default/files/Metadata%20Module.pdf> Accessed 11 June 2019.

International Organization for Standardization. 2013. *Information technology – Security techniques – Information security management systems – Requirements*. ISO/IEC 27001. <https://www.iso.org/standard/54534.html> Accessed 2 February 2020.

International Organization for Standardization. (2016). *Information and documentation records management*. ISO 15489-1.

<https://www.iso.org/standard/62542.html> Accessed 2 February 2020.

InterPARES Trust. 2016. *Social media and trust in government*.

https://interparestrust.org/docs/file/NA05_20161209_SocialMediaResearchPhase1_FinalReport_Final.pdf Accessed 20 April 2019.

InterPARES Trust. 2018. *Terminology*.

<https://interparestrust.org/terminology/term/record> Accessed 18 August 2019.

Jaeger, P.T., Bertot, J.C. and Shilton, K. 2012. *Information policy and social media: framing government citizen Web 2.0 interactions*.

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.7541&rep=rep1&type=pdf> Accessed 14 March 2019.

Jansen, W. and Grance, T. 2011. *Guidelines on security and privacy in public cloud computing*.

https://www.privacy.nl/uploads/cloud/security_cloud_dec_2011.pdf Accessed 19 February 2019.

Jeurgens, C. 2017. Threat of the data-flood: an accountability perspective in the era of ubiquitous computing. In: Smit, F., Glaudemans, A. and Jonker, R. eds. *Archives in liquid times*. 's-Gravenhage: Stichting Archiefpublicaties, pp. 229-246.

Karrim, A. 2020. *Minister to lay a charge over coronavirus fake news*.

<https://www.news24.com/SouthAfrica/News/minister-to-lay-a-charge-for-coronavirus-fake-news-20200325> Accessed 13 April 2020.

Ketelaar, E. 2017. Foreword. In: Smit, F., Glaudemans, A. and Jonker, R. eds. *Archives in liquid times*. 's-Gravenhage: Stichting Archiefpublicaties, p. vii.

Latham, R. 2014. *Information management advice 57 managing social media. Records part 1: Overview.*

<https://www.informationstrategy.tas.gov.au/Records-ManagementPrinciples/Document%20Library%20%20Tools/Advice%2057%20Managing%20Social%20Media%20Records%20Part%201%20-%20Overview.pdf> Accessed 2 November 2019.

Library of Congress. 2018. *Personal archiving: Preserving your digital memories.* <http://www.digitalpreservation.gov/personalarchiving/websites.html> Accessed 2 November 2019.

Litvinova, D. 2020. *Fake news or the truth? Russia cracks down on virus postings.* <https://apnews.com/dbbf02a747b11d8ffe3b07d5e33ff129> Accessed 13 April 2020.

Madhava, R. 2011. *10 Things to know about preserving social media.* http://content.arma.org/IMM/Libraries/SeptOct_2011_PDFs/IMM_0911_10_things_to_know_about_preserving_social_media.sflb.ashx Accessed 15 March 2019.

Masekoameng, M.F. 2018. Integration of social media records into enterprise content management at the South African Broadcasting Corporation in the Limpopo province of South Africa. Master's dissertation. Pretoria: University of South Africa.

Masilo, B. Seabo, B. 2015. Facebook: revolutionising electoral campaign in Botswana? *Journal of African Elections* 14(2): 110- 219

Mosweu, T. and Ngoepe, M. 2018. Governance of liquid communications in the Botswana public sector: neither restricted by time nor space. In: Chisita, C.T. and Rusero, A.M.M. eds. *Exploring the relationship between media, libraries, and archives.* Harrisburg, PA: IGI Global, pp. 53-69.

Mickoleit, A. 2014. *Social media use by governments: a policy primer to discuss trends, identify policy opportunities and guide decision makers: OECD Working Papers on Public Governance.* <http://dx.doi.org/10.1787/5jxrcmghmk0s-en> Accessed 1 July 2020.

Mitchetti, G. 2017. Provenance in the archives: the challenge of the digital. In: Smit, F., Glaudemans, A. and Jonker, R. eds. *Archives in liquid times.* 's-Gravenhage: Stichting Archiefpublicaties, pp. 229-246.

National Information Technology Development Agency. 2017. *Framework and guidelines for the use of social media platforms in government establishments*. http://nitda.gov.ng/wp-content/uploads/2012/11/MDAs-Social-Media-Guideline-D_eGDR-TA-Kem-Luk-Amend-3.pdf Accessed 3 March 2020.

Ngoepe, M. and Saurombe, A. 2016. Provisions for managing and preserving records created in networked environments in the archival legislative frameworks of selected member states of the Southern African Development Community. *Archives and Manuscripts* 44(1): 24-41.

Parer, D. 2002. *Archival legislation for commonwealth countries*. http://www.acarm.org/oid%5Cdownloads%5C4%5C1_1_3_41_05_PM_Legislation%20Report.pdf Accessed 13 March 2019.

Public Records Office Victoria. 2013. *Capturing records of social media posts*. https://prov.vic.gov.au/sites/default/files/2016-05/Social_Media_FS1.pdf Accessed 13 March 2019.

Rogers, C. 2009. Virtual authenticity: authenticity of digital records from theory to practice. Master's dissertation. Vancouver: University of British Columbia.

Rogers, C. 2015. Diplomats of born digital documents – considering documentary form in a digital environment. *Records Management Journal* 25: 6-20.

Smallwood, RF. 2014. *Information governance*. New Jersey: John Wiley & Sons.

Smit, F., Glaudemans, A. and Jonker, R. eds. 2017. *Archives in liquid times*. 's-Gravenhage: Stichting Archiefpublicaties.

Statistics Botswana. 2014. *Botswana household access and individual use of information & communication technologies – 2014*. <http://www.statsbots.org.bw/sites/default/files/publications/Botswana%20Access%20and%20Use%20of%20ICTs%202014%20Statistics.pdf> Accessed 25 June 2019.

Sunday Standard Reporter. 2016. Botswana has highest rates of Facebook use in Africa. *Sunday Standard Newspaper*, 29 March. <http://www.sundaystandard.info/botswana-has-highest-rates-facebook-use-africa> Accessed 25 June 2019.

The Standard. 2020. *20 years in jail for spreading fake coronavirus news*.
<https://www.thestandard.co.zw/2020/03/29/20-years-jail-spreading-fake-coronavirus-news/> Accessed 13 April 2020.

Thompson, S.D. 2016. *Preserving social media DPC technology watch report*.
<https://www.dpconline.org/docs/technology-watch-reports/1486-twr16-01/file>
Accessed 22 February 2019.

Vision 2016 Council. 2015. *Botswana performance report 2015*.
http://www.vision2016.co.bw/tempimg/media/mediac_189.pdf Accessed 25 June 2019.

VOA News. 2020. *Coronavirus puts Southeast Asian anti-fake news laws to test*.
<https://www.voanews.com/science-health/coronavirus-outbreak/coronavirus-puts-southeast-asian-anti-fake-news-laws-test> Accessed 13 April 2020.

Yeo, G. 2013. Trust and context in cyberspace. *Archives and records* 34(2): 214-234.

Yeo, G. 2015. Record(s). In Duranti, L. and Franks, P. eds. *Encyclopaedia of archival science*. New York: Rowman & Littlefield, pp. 79-81.

Zapata, D.D. 2013. *Liquid communication: how FC Barcelona is spreading sentiment Blaugrana one drop at a time*.
http://digitool.library.colostate.edu/webclient/eliveryManager/digitool_items/cs_u01_storage/2013/10/23/file_1/247896 Accessed 25 June 2019.